DETAILED ACTION

The instant application having Application No. 10/591276 filed on 8/31/06 is presented for examination by the examiner.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Specification

The disclosure is objected to because of the following informalities:

(i) proper headings need to be inserted.

Content of Specification

(a) Title of the Invention: See 37 CFR 1.72(a) and MPEP § 606. The title of the invention should be placed at the top of the first page of the specification unless the title is provided in an application data sheet. The title of the invention should be brief but technically accurate and descriptive, preferably from two to seven words may not contain more than 500 characters.

(b) Cross-References to Related Applications: See 37 CFR 1.78 and MPEP § 201.11.

(c) Statement Regarding Federally Sponsored Research and Development: See MPEP § 310.

(d) The Names Of The Parties To A Joint Research Agreement: See 37 CFR 1.71(g).

(e) Incorporation-By-Reference Of Material Submitted On a Compact Disc: The specification is required to include an incorporation-by-reference of electronic documents that are to become part of the permanent United States Patent and Trademark Office records in the file of a patent application. See 37 CFR 1.52(e) and MPEP § 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text were permitted as electronic documents on compact discs beginning on September 8, 2000.

(f) Background of the Invention: See MPEP § 608.01(c). The specification should set forth the Background of the Invention in two parts:

(1) Field of the Invention: A statement of the field of art to which the invention pertains. This statement may include a paraphrasing of the applicable U.S. patent classification definitions of the subject matter of the claimed invention. This item may also be titled "Technical Field."

(2) Description of the Related Art including information disclosed under 37 CFR 1.97 and 37 CFR 1.98: A description of the related art known to the applicant and including, if applicable, references to specific related art and problems involved in the prior art which are solved by the applicant's invention. This item may also be titled "Background Art."

(g) Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.

(h) Brief Description of the Several Views of the Drawing(s): See MPEP § 608.01(f). A reference to and brief description of the drawing(s) as set forth in 37 CFR 1.74.

(i) Detailed Description of the Invention: See MPEP § 608.01(g). A description of the preferred embodiment(s) of the invention as required in 37 CFR 1.71. The description should be as short and specific as is necessary to describe the invention adequately and accurately. Where

elements or groups of elements, compounds, and processes, which are conventional and generally widely known in the field of the invention described and their exact nature or type is not necessary for an understanding and use of the invention by a person skilled in the art, they should not be described in detail. However, where particularly complicated subject matter is involved or where the elements, compounds, or processes may not be commonly or widely known in the field, the specification should refer to another patent or readily available publication which adequately describes the subject matter.

(j) Claim or Claims: See 37 CFR 1.75 and MPEP § 608.01(m). The claim or claims must commence on separate sheet or electronic page (37 CFR 1.52(b)(3)). Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation. There may be plural indentations to further segregate subcombinations or related steps. See 37 CFR 1.75 and MPEP § 608.01(i)-(p).

(k) Abstract of the Disclosure: See MPEP § 608.01(f). A brief narrative of the disclosure as a whole in a single paragraph of 150 words or less commencing on a separate sheet following the claims. In an international application which has entered the national stage (37 CFR 1.491(b)), the applicant need not submit an abstract commencing on a separate sheet if an abstract was published with the international application under PCT Article 21. The abstract that appears on the cover page of the pamphlet published by the International Bureau (IB) of the World Intellectual Property Organization (WIPO) is the abstract that will be used by the USPTO. See MPEP § 1893.03(e).

(l) Sequence Listing, See 37 CFR 1.821-1.825 and MPEP §§ 2421-2431. The requirement for a sequence listing applies to all sequences disclosed in a given application, whether the sequences are claimed or not. See MPEP § 2421.02.

(ii) The reference to Patent Document 1 on page 1 of the specification should be removed and incorporated by reference, as opposed to the reference call on line 16.

Appropriate correction is required.

Claim Objections

Claim 6 is objected to because of the following informalities: typo “potable" [portable].

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 16 and 17 are rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, per se. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor is it a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, function descriptive material per se.

Descriptive material can be characterized as either “functional descriptive material” or “nonfunctional descriptive material.” Both types of “descriptive material” are non-statutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").See MPEP 2106.01 [R-6].

Claim 16 is directed to a software program which does not fall under any statutory classes. Claim 17 is a program on a computer-readable recording medium. However only when the computer-readable recording medium is inserted into a computer and executed by a computer does it become statutory subject matter. The claim lacks this relationship.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 5 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim, the public key is referenced but it is unclear which public key is being addressed. The public key could be any of the device's public keys or interpreted to mean a public key of the source server. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, and 14-17 are rejected under 35 U.S.C. 102(b) as being anticipated by USP Application Publication 2002/0049654 to Thomas et al., hereinafter Thomas.

As per claims 1, 14, 15, 16, and 17, Thomas teaches an information security apparatus [and method] that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the information security apparatus comprising :

a private key generating unit operable to generate a private key (0012);

a parameter receiving unit operable to receive parameters which respectively determine conditions [licenses] (0054); and

a public key generating unit operable to generate, with use of the private key, public keys from sets of integers that satisfy the conditions [licenses] determined by the parameters (0012). These parameters are understood to be the setup parameters agreed upon between any two entities needed to perform public/private key communication.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of prior art document, "Receiver Anonymity via Incomparable Public Keys" by Waters, Felten, and Sahai, hereinafter Waters.

As per claim 2, Thomas teaches the information security apparatus is connected to servers via a network (0007), and

the parameters are received from the servers respectively and are different from each other (0054). Thomas teaches that a single client can communicate/enroll with more than one server (0007). There is no reason to believe that if the clearinghouse servers are different that all the servers would choose the same parameters to initiate asymmetrical key encryption. Thomas is silent in disclosing the public key generating unit generates public keys which are different from each other, with use of the respective parameters. Waters teaches the public key generating unit generates public keys which are different from each other, with use of the respective parameters (section 1.2). Waters teaches a system whereby a device wanting to communicate securely

between many different servers, can create many public keys corresponding to one private key. The advantage here is the system leaks less valuable information to an outsider by using anonymous public keys. In Thomas' system the devices do not inherently trust the servers. Using different public keys with each server would augment this type of network because the user may not know if he can trust the server in the future. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the multiple public keys of Waters into the system of Thomas because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in the their respective functions, and the combination would have yielded predictable results.

As per claim 3, Thomas teaches a public key transmission unit operable to transmit the public keys to respective source servers that are sources of the respective parameters (0012);

a public key certification receiving unit operable to receive public key certifications from the respective servers, each public key certification including each public key and a signature of each server (0035); and

a key storage unit operable to store the private key and the public key certifications (0035). Certificates are inherently signed with the private key of the publisher. Both the private key and the certificates are stored by the device.

As per claim 4, Thomas teaches a contents request unit operable to read out one of the public key certifications from the key storage unit, and transmit a contents request

that includes the read-out public key certification to a source server that has issued the read-out public key certification (0008); and

a contents acquiring unit operable to acquire contents from the source server in a safe and reliable manner with use of the private key and the public key included in the read-out public key certification (0011).

As per claim 5, Thomas teaches an authenticating unit operable to transmit, to the source server, signature data that is generated with use of the private key and to be authenticated by the source server with use of the public key, and authenticate the source server (0008 and 0011);

a key sharing unit operable to share key information with the source server if the authentication performed by the authentication unit succeeds (0012);

a receiving unit operable to receive encrypted contents, which are encrypted based on the key information, from the source server (0012); and

a decrypting unit operable to decrypt the encrypted contents based on the key information (0012).

Claims 6, 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas and Waters as applied to claim 3 above, and further in view of USP 7124938 to Marsh.

As per claim 6, Thomas and Waters are silent in disclosing the key storage unit is a portable memory card that is inserted in the information security apparatus, the public key generating unit writes the private key and the public key certifications into the

potable memory card, and the portable memory card includes a secure storage area that is secure against tampering and cryptanalysis from outside, and stores the private key in the secure storage area. Marsh teaches the key storage unit is a portable memory card that is inserted in the information security apparatus (Fig. 3, 246), the public key generating unit writes the private key and the public key certifications into the potable memory card (col. 9, line 65-col. 10, line 2), and

the portable memory card includes a secure storage area that is secure against tampering and cryptanalysis from outside, and stores the private key in the secure storage area (col. 9, lines 65-66). The use of smart cards is well-known in the art of cryptography. Smart cards are known to a safe place for storing key and other sensitive data in computing systems. The claim would have been obvious because the use of smart cards for improving a particular class of security devices was part of the ordinary capabilities of a person of ordinary skill in the art, in view of the teaching of Marsh for improvement in other situations.

As per claim 7, Thomas and Waters are silent in disclosing a memory card authenticating unit operable to authenticate the memory card when the memory card is inserted into the information security apparatus; and

a write-inhibit unit operable to inhibit the public key generating unit from writing the private key and the public key certifications into the memory card if the authentication performed by the memory card authenticating unit fails. Examiner supplies the same rationale for combining the use of smart cards into the teaching of Thomas and Waters. Marsh teaches authentication the smart card with the device and no providing services

with the smart if authentication fails (col. 15, line 65-col. 16, line 5). The claim would have been obvious because the use of smart card authentication for improving a particular class of security devices was part of the ordinary capabilities of a person of ordinary skill in the art at the time of the invention, in view of the teaching of Marsh for improvement in other situations.

Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of USP 6,212,277 to Miyaji.

As per claim 8, Thomas is silent in disclosing that security of the information security apparatus is based on an elliptic curve discrete logarithm problem,

the parameter receiving unit receives parameters that constitute an elliptic curve, and the public key generating unit generates the public keys by performing, for each parameter, a multiplication with use of the elliptic curve on the private key.

Miyaji teaches security of the information security apparatus (Fig. 2, 200) is based on an elliptic curve discrete logarithm problem (Fig. 2, 230),

the parameter receiving unit receives parameters that constitute an elliptic curve (Fig. 2, 210),

and the public key generating unit generates the public keys by performing, for each parameter, a multiplication with use of the elliptic curve on the private key (Fig. 2, 230). One of ordinary skill in the art knows that the elliptic curve discrete logarithm can be used in the field of asymmetric key cryptography. Therefore a simple substitution of

one known, equivalent element for another to obtain predictable results is obvious. The claim would have been obvious because the substitution of one known element for another would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

As per claim 9, Thomas is silent in disclosing the private key generating unit generates a private key SK, the parameter receiving unit receives sets of parameters, each including a and b constituting the elliptic curve y2=x3+ax+b, a prime number p, and a base point G on the elliptic curve, and
the public key generating unit generates the public keys by calculating SK*G(mod p) for each set of the parameters. Miyaji teaches the private key generating unit generates a private key SK (Fig. 7, S401), the parameter receiving unit receives sets of parameters (Fig. 2, 210) each including a and b constituting the elliptic curve y2=x3+ax+b, a prime number p, and a base point G on the elliptic curve (Fig. 7, S434), and
the public key generating unit generates the public keys by calculating SK*G(mod p) for each set of the parameters (Fig. 7, S404). This claim further expounds on the elliptic curve algorithm which is known and taught by Miyaji. Examiner supplies the same rationale for combining as reciting in the rejection of claim 8.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of USP 6,134,325 to Vanstone et al., hereinafter Vanstone.

As per claim 10, Thomas teaches the use of a public/private key system but does not explicitly teach the RSA cryptosystem. Claim recites some of the details of the RSA cryptosystem and how it applies in the claimed invention. Vanstone teaches the RSA and in particular, security of the information security apparatus is based on an RSA cryptosystem (col. 1, lines 34-39),

the private key generating unit generates a private key d (col. 1, lines 38), the parameter receiving unit receives sets of prime numbers (P, Q) as the parameters (col. 1, line 35), and

the public key generating unit generates sets of the public keys (N, e) by calculating N=PQ and further calculating e from ed≡mod(P-l)(Q-l), for each set of the prime numbers (col. 1, lines 35-39). One of ordinary skill in the art knows that RSA can be used in the field of asymmetric key cryptography. Therefore a simple substitution of one known, equivalent element for another to obtain predictable results is obvious. The claim would have been obvious because the substitution of one known element for another would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Claims 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas in view of Marsh.

As per claim 11, Thomas teaches an information security apparatus that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the information security apparatus

comprising :

a private key generating unit operable to generate a private key (0012);

a parameter receiving unit operable to receive parameters which respectively determine conditions [licenses] (0054); and

a public key generating unit operable to generate, with use of the private key, public keys from sets of integers that satisfy the conditions [licenses] determined by the parameters (0012). These parameters are understood to be the setup parameters agreed upon between any two entities needed to perform public/private key communication. Thomas is silent in disclosing a private key storage unit operable to store the private key in an area that is secure against tampering and cryptanalysis from outside. Marsh teaches a private key storage unit that is secure against tampering and cryptanalysis from outside, and stores the private key in the secure storage area (col. 9, lines 65-66). The use of smart cards is well-known in the art of cryptography. Smart cards are known to a safe place for storing key and other sensitive data in computing systems. The claim would have been obvious because the use of smart cards for improving a particular class of security devices was part of the ordinary capabilities of a person of ordinary skill in the art, in view of the teaching of Marsh for improvement in other situations.

Claims 12 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas and Marsh as applied to claim 11 above, and further in view of Waters.

As per claim12, Thomas teaches a terminal device that is connected to servers via a network (0007), the parameters are received from the servers respectively via the terminal device and are different from each other (0054). These parameters are understood to be the setup parameters agreed upon between any two entities needed to perform public/private key communication. There is no reason to believe that if the clearinghouse servers are different that all the servers would choose the same parameters to initiate asymmetrical key encryption.

Thomas is silent in disclosing a memory card is inserted into the terminal device. Examiner supplies the same rationale for combining the use of smart cards into the teaching of Thomas. Marsh teaches the key storage unit is a portable memory card that is inserted in the information security apparatus (Fig. 3, 246). The use of smart cards is well-known in the art of cryptography. Smart cards are known to a safe place for storing key and other sensitive data in computing systems. The claim would have been obvious because the use of smart cards for improving a particular class of security devices was part of the ordinary capabilities of a person of ordinary skill in the art, in view of the teaching of Marsh for improvement in other situations.

Thomas is silent in disclosing the public key generating unit generates public keys which are different from each other, with use of the respective parameters. Waters teaches the public key generating unit generates public keys which are different from each other, with use of the respective parameters (section 1.2). Waters teaches a system whereby a device wanting to communicate securely between many different

servers, can create many public keys corresponding to one private key. The advantage here is the system leaks less valuable information to an outsider by using anonymous public keys. In Thomas' system the devices do not inherently trust the servers. Using different public keys with each server would augment this type of network because the user may not know if he can trust the server in the future. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the multiple public keys of Waters into the system of Thomas because all of the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in the their respective functions, and the combination would have yielded predictable results.

As per claim 13, Thomas teaches the memory card acquires, in a safe and secure manner, contents from each server via the terminal device, with use of the private key and the public keys (0011).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431